Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
  - Capturix ScanShare Password Disclosure
  - ClearSwift MIMEsweeper Arbitrary Code Injection
  - Comersus Cart Cross Site Scripting or SQL Injection
  - CartWIZ Cross Site Scripting or SQL Injection
  - Hosting Controller Credit Modification or Account Creation
  - Dragonfly Commerce SQL Injection or Price Modification
  - **K-Meleon Denial of Service (Update)**
  - MailEnable Professional Arbitrary Code Execution
  - McAfee Security Management System Elevated Privileges or Cross Site Scripting
  - MS ASP.NET Denial of Service
  - JView Profiler Arbitrary Code Execution
  - MSN Messenger Protocol Denial of Service
  - Microsoft MSRPC Information Disclosure
  - Microsoft Outlook Express Information Disclosure or System Crash
  - Microsoft Windows Color Management Module Buffer Overflow or Arbitrary Code Execution
  - Microsoft Word Buffer Overflow or Arbitrary Code Execution
  - PrivaShare Denial of Service
  - WMailserver Information Disclosure
  - Web Wiz Forums Information Disclosure
- UNIX / Linux Operating Systems
  - Backup Manager File Permissions
  - Blog Torrent Password Disclosure
  - Debian File Permission
  - Elmo Arbitrary File Overwrite
  - GNATS Arbitrary File Overwriting
  - GNU MailWatch Arbitrary Code Execution
  - Heartbeat Arbitrary File Overwrite
  - **IBM AIX Multiple Buffer Overflows (Update)**
  - IBM ftpd Denial of Service
  - SecureLinx SLC Console Manager File Disclosure
  - MediaWiki Cross Site Scripting
  - MMS Ripper Arbitrary Code Execution
  - Bugzilla Private Summary Disclosure or Flag Modification
  - Multiple Vendors dhcpcd Denial of Service
  - Linux Kernel Race Condition and Buffer Overflow
  - PunBB SQL Injection or Arbitrary Code Execution
  - SGI ARShell Elevated Privileges
  - TikiWiki Arbitrary Code Execution
  - XPVM Arbitrary File Overwrite
- Multiple Operating Systems
  - Ampache Arbitrary Code Execution
  - phpWebSite SQL Injection or Arbitrary Code Execution
  - eTrust SiteMinder Cross Site Scripting
  - Cisco CallManager Denial of Service or Arbitrary Code Execution
  - Cisco 7940/7960 SIP Packet Spoofing
  - Dansie Shopping Cart Variables Disclosure
  - Download Protect Information Disclosure
  - BIG-IP Authentication Bypassing
  - BudgeTone 100 SIP Packet Spoofing
  - Tivoli Management Framework Endpoint Service (lcfd) Denial of Service
  - Id Board SQL Injection
  - **Interspire ArticleLive Multiple Remote Vulnerabilities (Update)**
  - iPhotoAlbum Arbitrary Command Execution
  - Jinzora Arbitrary File Inclusion
  - Moodle Vulnerabilities
  - Nokia Affix BTFTP Arbitrary Code Execution
  - Novell Netmail Script Insertion Vulnerability
  - phpSecurePages Arbitrary Code Execution
  - PHPAuction Cross-Site Scripting, SQL Injection, or Authentication Bypassing
  - phpSlash Account Hijacking or Elevated Privileges
  - phpWishList Unauthorized Administrative Access

- PhpXmail Authentication Bypassing
- pngren Arbitrary Command Execution
- PhotoGal Arbitrary Code Execution
- Simple PHP Blog Password Exposure
- SPiD Arbitrary File Inclusion
- Squito Gallery Arbitrary Commands Execution
- USANet Remote Command Execution
- Xerox WorkCentre Pro Authentication Bypassing, Unauthorized Files Access, Web Page Modification, or Denial of Service
- PPA Arbitrary Command Execution
- Zlib Arbitrary Code Execution

Wireless

Recent Exploit Scripts/Techniques

Trends
Viruses/Trojans

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Capturix Technologies ScanShare 1.06	A vulnerability has been reported in ScanShare that could let local malicious users disclose passwords. No workaround or patch available at time of publishing. There is no exploit code required.	Capturix ScanShare Password Disclosure CAN-2005-2209	Medium	Security Tracker, Alert ID: 1014409, July 7, 2005
ClearSwift MIMEsweeper 5.1	A vulnerability has been reported in MIMEsweeper that could let remote malicious users inject arbitrary code. Vendor update available: http://www.clearswift.com/support/msw/patch_MswWeb.aspx There is no exploit code required.	ClearSwift MIMEsweeper Arbitrary Code Injection	High	Security Tracker Alert ID: 1014456, July 12, 2005
Comersus Comersus Cart 6.0.41	An input validation vulnerability has been reported in Comersus Cart that could let remote malicious users perform Cross-Site scripting or SQL injection attacks. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Comersus Cart Cross Site Scripting or SQL Injection CAN-2005-2190 CAN-2005-2191	High	Security Tracker, Alert ID: 1014419, July 7, 2005

Elemental Software CartWiz 1.20	An input validation vulnerability has been reported in CartWiz that could let remote malicious users perform Cross-Site Scripting or SQL injection attacks. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	CartWIZ Cross Site Scripting or SQL Injection CAN-2005-2206 CAN-2005-2207	High	Security Tracker, Alert ID: 1014418, July 7, 2005
Hosting Controller Hosting Controller 6.1 Hotfix 2.1	Multiple vulnerabilities have been reported in Hosting Controller (AccountActions.asp) that could let remote authenticated, malicious users to modify their credit limit or create new accounts. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Hosting Controller Credit Modification or Account Creation CAN-2005-2219	Medium	Security Tracker Alert ID: 1014443, 1014446, July 11, 2005
Incredible Interactive Dragonfly Commerce	A vulnerability has been reported in Dragonfly Commerce that could let remote malicious users perform SQL injection and price data modification. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Dragonfly Commerce SQL Injection or Price Modification CAN-2005-2220 CAN-2005-2221	High	Security Tracker Alert ID: 1014451, July 12, 2005
K-Meleon K-Meleon Browser 0.9	An empty javascript function processing vulnerability has been reported in K-Meleon Browser that could let remote malicious users perform a Denial of Service. As a workaround disable Javascript. A Proof of Concept exploit has been published.	K-Meleon Denial of Service CAN-2005-2114	Low	**Security Tracker Alert ID: 1014372, July 4, 2005** **Advisory erroneously referenced.**
MailEnable MailEnable Professional 1.6	A vulnerability has been reported in MailEnable Professional that could let remote malicious users execute arbitrary code or a Denial of Service during authentication. Vendor fix available: http://www.mailenable.com/download.asp Currently we are not aware of any exploits for this vulnerability.	MailEnable Professional Arbitrary Code Execution CAN-2005-2222 CAN-2005-2223	High	Security Tracker, Alert ID: 1014427, July 8, 2005
McAfee Security Management System	Multiple vulnerabilities have been reported in Security Management System that could let remote authenticated, malicious users obtain elevated privileges or perform Cross-Site Scripting attacks. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	McAfee Security Management System Elevated Privileges or Cross Site Scripting CAN-2005-2186 CAN-2005-2187	High	Secunia, Advisory: SA15961, July 7, 2005
Microsoft ASP .NET	An input validation vulnerability has been reported in ASP .NET that could let remote malicious users perform a Denial of Service. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	ASP.NET Denial of Service CAN-2005-2224	Low	Secunia, Advisory: SA16005, July 12, 2005
Microsoft JView Profiler	A vulnerability has been reported in JView Profiler that could let remote malicious users execute arbitrary code. Vendor updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-037.mspx There is no exploit code required; however, a Proof of Concept exploit has been published.	JView Profiler Arbitrary Code Execution CAN-2005-2087	High	Microsoft Security Bulletin MS05-037, July 12, 2005 USCERT, Vulnerability Note VU#939605, July 12, 2005

Microsoft MSN Messenger Protocol	A vulnerability has been reported in MSN Messenger Protocol that could let remote malicious users perform a Denial of Service. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	MSN Messenger Protocol Denial of Service CAN-2005-2225	Low	Security Tracker Alert ID: 1014444, July 11, 2005
Microsoft MSRPC	Multiple vulnerabilities have been reported in MS remote procedure call that could let remote malicious users disclose information. Upgrade to Update RollUp 1: http://www.microsoft.com/downloads/details.aspx?amp;displaylang=en&familyid=c0a2ca36-1179-431c-80e6-60a494d3823d&displaylang=en Currently we are not aware of any exploits for this vulnerability.	Microsoft MSRPC Information Disclosure CAN-2005-2150	Medium	Security Focus, 14177, 14178, July 7, 2005
Microsoft Outlook Express 6.0	Multiple vulnerabilities have been reported in Outlook Express that could let a remote malicious user disclose information or crash the system. Vendor update available: http://support.microsoft.com/default.aspx/kb/900930/EN-US/ Some included vulnerabilities are no exploit code required, others may have published exploits.	Microsoft Outlook Express Information Disclosure or System Crash CAN-2005-2226	Medium	Security Focus, 14225, July 12, 2005
Microsoft Windows Color Management Module	A vulnerability has been reported in Windows Color Management Module that could let remote malicious users cause a buffer overflow, execute arbitrary code, or take complete control of a system. Vendor updates available: http://www.microsoft.com/technet/security/bulletin/ms05-036.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Color Management Module Buffer Overflow or Arbitrary Code Execution CAN-2005-1219	High	Microsoft Security Bulletin MS05-036, July 12, 2005 USCERT, Vulnerability Note VU#720742, July 12, 2005
Microsoft Word	A vulnerability has been reported in Word that could let remote malicious users cause a buffer overflow or execute arbitrary code. Vendor updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-035.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Word Buffer Overflow or Arbitrary Code Execution CAN-2005-0564	High	Microsoft Security Bulletin MS05-035, July 12, 2005 USCERT, Vulnerability Note VU#218621, July 12, 2005
PrivaShare PrivaShare 1.3	A vulnerability has been reported in PrivaShare that could let remote malicious users perform a Denial of Service. No workaround or patch available at time of publishing. An exploit has been published.	PrivaShare Denial of Service CAN-2005-2208	Low	Secunia, Advisory: SA15933, july 7, 2005
Softiacom WMailserver 1.0	A vulnerability has been reported in WMailserver that could let local malicious users disclosure information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	WMailserver Information Disclosure CAN-2005-2227	Medium	Security Focus, 14212, July 11, 2005
Web Wiz Web Wiz Forums 7.9, 8.0	A vulnerability has been reported in Web Wiz Forums that could let remote malicious users disclose information. No workaround or patch available at time of publishing. There is no exploit code required.	Web Wiz Forums Information Disclosure CAN-2005-2228	Medium	Security Focus, 14207, July 11, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Backup Manager Backup Manager 0.5.8a	Multiple file permission vulnerabilities have been reported in Backup Manager that could let local malicious users obtain elevated privileges or view/ modify the repository. Update to version 0.5.8b: http://www.sukria.net/packages/backup-manager/sources/backup-manager-0.5.8b.tar.gz There is no exploit code required.	Backup Manager File Permissions CAN-2005-2211 CAN-2005-2212	Medium	Secunia, Advisory: SA15989, July 11, 2005
blogtorrent.com Blog Torrent 0.92	A vulnerability has been reported in Blog Torrent that could let remote malicious users disclose hashed passwords. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Blog Torrent Password Disclosure CAN-2005-2229	Medium	Security Tracker Alert ID: 1014449, July 11, 2005
Debian Linux 3.1	A 'apt.conf' permission vulnerability has been reported in Debian that could let local malicious users access sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	Debian File Permission CAN-2005-2214	Medium	Secunia, Advisory: SA15955, July 7, 2005
Elmo Elmo 1.3.2	An insecure file creation vulnerability has been reported in Elmo that could let local users arbitrarily overwrite files. No workaround or patch available at time of publishing. There is no exploit code required.	Elmo Arbitrary File Overwrite CAN-2005-2230	Medium	Secunia, Advisory: SA15977, July 12, 2005
GNATS GNATS 4.1.0	A vulnerability has been reported in GNATS that could let local malicious uses overwrite arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	GNATS Arbitrary File Overwriting CAN-2005-2180	Medium	Secunia, Advisory: SA15963, July 7, 2005
GNU MailWatch For MailScanner 1.0	An XML-RPC for PHP vulnerability has been reported in MailWatch For MailScanner that could let remote malicious users execute arbitrary code. Update to version 1.0.1: http://sourceforge.net/project/showfiles.php?group_id=87163 There is no exploit code required.	MailWatch Arbitrary Code Execution CAN-2005-1921	High	Secunia, Advisory: SA15947, July 7, 2005
High Availability Linux Project Heartbeat 1.2.3	An insecure file creation vulnerability has been reported in Heartbeat that could let local users arbitrarily overwrite files. No workaround or patch available at time of publishing. There is no exploit code required.	Heartbeat Arbitrary File Overwrite CAN-2005-2231	Medium	Secunia Advisory: SA16039, July 12, 2005
IBM AIX 5.3	Buffer overflow vulnerabilities have been reported in the 'invscout,' 'paginit,' 'diagTasksWebSM,' 'getlvname,' and 'swcons' commands and multiple 'p' commands, which could let a malicious user execute arbitrary code, potentially with root privileges. IBM has released an advisory (IBM-06-10-2005) to address this and other issues. **Vendor fix available:** **http://www-1.ibm.com/servers/eserver/support/pseries/aixfixes.html** There is no exploit code required; however, a Proof	IBM AIX Multiple Buffer Overflows CAN-2005-2232 CAN-2005-2233 CAN-2005-2234 CAN-2005-2235 CAN-2005-2236 CAN-2005-2237	High	Security Tracker Alert, 1014132, June 8, 2005 IBM Security Advisory, IBM-06-10-2005, June 10, 2005 **Security Focus, 13909, July 7, 2005**

	of Concept exploit has been published.			
IBM ftpd	A timeout vulnerability has been reported in ftpd, on IBM AIX, that could let remote malicious users perform a Denial of Service. Vendor fix available: ftp://aix.software.ibm.com/aix/efixes/security/ftpd_ifix.tar.Z Currently we are not aware of any exploits for this vulnerability.	IBM ftpd Denial of Service CAN-2005-2238	Low	Security Tracker, Alert ID: 1014421, July 8, 2005 USCERT, Vulnerability Note VU#118125, July 7, 2005
Lantronix SecureLinx SLC Console Manager	A file access vulnerability has been reported in SecureLinx SLC Console Manager that could let remote malicious users access sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	SecureLinx SLC Console Manager File Disclosure CAN-2005-2189	Medium	Secunia, Advisory: SA15979, July 8, 2005
MediaWiki MediaWiki 1.4.5	A vulnerability has been reported in MediaWiki that could let remote malicious users perform Cross-Site Scripting attacks. Update to version 1.4.6: http://sourceforge.net/project/showfiles.php?group_id=34373 There is no exploit code required.	MediaWiki Cross Site Scripting CAN-2005-2215	High	Security Focus, 14181, July 7, 2005
MMS Ripper MMS Ripper 0.6	A buffer overflow vulnerability has been reported in MMS Ripper that could let remote malicious users to execute arbitrary code. Update to version 0.6.4: http://nbenoit.tuxfamily.org/projects.php?rq=mmsrip Currently we are not aware of any exploits for this vulnerability.	MMS Ripper Arbitrary Code Execution CAN-2005-2213	High	Secunia, Advisory: SA15987, July 11, 2005
Mozilla Bugzilla 2.18.2	A vulnerability has been reported in Bugzilla that could let remote malicious users disclose private summaries or modify flags. Vendor fix available: http://www.bugzilla.org/download.html There is no exploit code required.	Bugzilla Private Summary Disclosure or Flag Modification CAN-2005-2173 CAN-2005-2174	Medium	Security Tracker, Alert ID: 1014428, July 8, 2005
Multiple Vendors dhcpcd 1.3.22	A vulnerability has been reported in dchpcd that could let a remote user perform a Denial of Service. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	dhcpcd Denial of Service CAN-2005-1848	Low	Secunia, Advisory: SA15982, July 11, 2005
Multiple Vendors Linux Kernel 2.4, 2.6	A race condition in ia32 emulation, vulnerability has been reported in the Linux Kernel that could let local malicious users obtain root privileges or create a buffer overflow. Patch Available: http://kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.32-pre1.bz2 Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Race Condition and Buffer Overflow CAN-2005-1768	High	Security Focus, 14205, July 11, 2005
PunBB PunBB 1.2.5	An input validation vulnerability has been reported in PunBB that could let remote malicious users execute arbitrary code or perform SQL injection attacks. Update to version 1.2.6: http://www.punbb.org/download/ There is no exploit code required; however, a Proof of Concept exploit has been published.	PunBB SQL Injection or Arbitrary Code Execution CAN-2005-2193	High	Security Tracker, Alert ID: 1014420, July 8, 2005
SGI SGI ArrayD ARShell 3.0, 4.0	A vulnerability has been reported in SGI ArrayD ARShell that could let remote malicious users obtain elevated root privileges. Vendor patches available: http://support.sgi.com/	SGI ARShell Elevated Privileges CAN-2005-1859	High	Security Focus, 14218, July 12, 2005

	Currently we are not aware of any exploits for this vulnerability.			
TikiWiki TikiWiki 1.x	A vulnerability has been reported in TikiWiki that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	TikiWiki Arbitrary Code Execution CAN-2005-1921	High	Secunia, Advisory: SA15944, July 7, 2005
XPVM XPVM 1.2.5	An insecure file creation vulnerability has been reported in XPVM that could let local malicious users arbitrarily overwrite files. No workaround or patch available at time of publishing. There is no exploit code required.	XPVM Arbitrary File Overwrite CAN-2005-2240	Medium	Secunia Advisory: SA16040, July 12, 2005

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Ampache Ampache 3.3.1	An XML-RPC for PHP vulnerability has been reported in Ampache that could let remote malicious users execute arbitrary code. Update to version 3.3.1.2: http://www.ampache.org/download.php There is no exploit code required.	Ampache Arbitrary Code Execution CAN-2005-1921	High	Secunia, Advisory: SA15957, July 8, 2005
Appalachian State University phpWebSite 0.10.1	Multiple vulnerabilities have been reported in phpWebSite that could let remote malicious users perform SQL injection or execute arbitrary code. Vendor Patch Available: http://www.phpwebsite.appstate.edu/index.php?module=announce&ANN_user_op=view&ANN_id=989 There is no exploit code required; however, a Proof of Concept exploit has been published.	phpWebSite SQL Injection or Arbitrary Code Execution CAN-2005-1921	High	Secunia, Advisory: SA15958, SA16001, July 8, 2005
CA Computer Associates (Netegrity) eTrust SiteMinder 5.5	An input validation vulnerability has been reported in eTrust SiteMinder (smpwservicescgi.exe) that could let remote malicious users perform Cross-Site Scripting attacks No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	eTrust SiteMinder Cross-Site Scripting CAN-2005-2204	High	Security Tracker, Alert ID: 1014433, July 9, 2005
Cisco Systems CallManager V3.3	Multiple vulnerabilities have been reported in CallManager that could let remote malicious users perform Denial of Service or arbitrary code execution. Vendor updates available: http://www.cisco.com/en/US/products/products_security_advisory09186a00804c0c26.shtml Currently we are not aware of any exploits for this vulnerability.	Cisco CallManager Denial of Service or Arbitrary Code Execution CAN-2005-2241 CAN-2005-2242 CAN-2005-2243 CAN-2005-2244	High	Security Focus, 14227, July 12, 2005
Cisco Systems Cisco 7940 & 7960 Series Phones	A vulnerability has been reported in Cisco 7940 & 7960 Series Phones that could let remote malicious users spoof SIP notify messages packets. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Cisco 7940/7960 SIP Packet Spoofing CAN-2005-2181	Medium	Security Tracker, Alert ID: 1014406, July 6, 2005

Dansie Dansie Shopping Cart	A vulnerability has been reported in Dansie Shopping Cart that could let remote malicious users disclose the variable file. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Dansie Shopping Cart Variables Disclosure CAN-2005-2217	Medium	Security Tracker, Alert ID: 1014396, July 6, 2005
Download Protect Download Protect 1.0.2b	An input validation vulnerability has been reported in Download Protect that could let remote malicious users disclose sensitive information. Update to version 1.0.3: http://php.reinsveien.com/DP/download.php There is no exploit code required.	Download Protect Information Disclosure CAN-2005-2248	Medium	Secunia, Advisory: SA16003, July 11, 2005
F5 Big-IP 9.0.2-9.1	A SSl authentication vulnerability has been reported in Big-IP that could let remote malicious users bypass authentication. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	BIG-IP Authentication Bypassing CAN-2005-2245	Medium	Secunia, Advisory: SA16008, July 12, 2005
Grandstream Networks BudgeTone 100 Series Phones	A vulnerability has been reported in BudgeTone 100 Series Phones that could let remote malicious users spoof SIP-notify-messages packets. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	BudgeTone 100 SIP Packet Spoofing CAN-2005-2182	Medium	Security Tracker, Alert ID: 1014407, July 6, 2005
IBM Tivoli Management Framework Endpoint Service (lcfd) 4.1.1	A vulnerability has been reported in Tivoli Management Framework Endpoint Service (lcfd) that could let remote malicious users perform a Denial of Service. Vendor patch available: http://www-1.ibm.com/support/docview.wss?uid=swg21210334 There is no exploit code required.	Tivoli Management Framework Endpoint Service (lcfd) Denial of Service CAN-2005-2170	Low	IBM Flash Alert, Reference #: 1210334, July 7, 2005
Id Team Id Board 1.1.3	An input validation vulnerability has been reported in Id Board that could let a remote malicious user perform SQL injection attacks. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Id Board SQL Injection CAN-2005-2197	High	Secunia, Advisory: SA15976, July 11, 2005
Interspire ArticleLive 2005	Multiple vulnerabilities have been reported which could let a remote malicious user obtain administrative access and execute arbitrary HTML and script code. **Update to ArticleLive 2005.0.5: http://www.interspire.com/articlelive/** There is no exploit code required; however, a Proof of Concept exploit has been published.	Interspire ArticleLive Multiple Remote Vulnerabilities CAN-2005-1482 CAN-2005-1483	High	Security Focus, 13493, May 4, 2005 **Security Focus, 13493, July 7, 2005**
iPhoto Album iPhotoAlbum 1.1	An include file vulnerability has been reported in IPhotoAlbum Gallery that could let remote malicious users execute arbitrary commands. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	iPhotoAlbum Arbitrary Command Execution CAN-2005-2246	High	Security Tracker Alert ID: 1014448, July 11, 2005
Jinzora Jinzora 2.0.1	A file inclusion vulnerability has been reported in Jinzora that could allow a remote malicious user to include arbitrary files. Update to version 2.1: http://www.jinzora.org/pages.php?pn=downloads	Jinzora Arbitrary File Inclusion CAN-2005-2249	Medium	Secunia, Advisory: SA15952, July 7, 2005

	There is no exploit code required.			
Moodle Moodle 1.5.1	Multiple vulnerabilities have been reported in Moodle that could let users perform unknown actions. Vendor fix available: http://download.moodle.org/ Currently we are not aware of any exploits for this vulnerability.	Moodle Vulnerabilities CAN-2005-2247	Not Specified	Security Tracker Alert ID: 1014453, July 12, 2005
Nokia Affix BTFTP	A buffer overflow vulnerability has been reported in Affix BTFTP that could let remote malicious users execute arbitrary code. Vendor patch available: Affix_320_sec.patch http://affix.sourceforge.net/affix_320_sec.patch Affix_212_sec.patch http://affix.sourceforge.net/affix_212_sec.patch An exploit has been published.	Nokia Affix BTFTP Arbitrary Code Execution	High	Security Focus, 14230, July 12, 2005
Novell NetMail 3.5	A vulnerability has been reported in NetMail that could let remote malicious users to insert scripts into mail. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Novell Netmail Script Insertion Vulnerability CAN-2005-2176	High	Secunia, Advisory: SA15962, July 8, 2005
PHP Secure Pages PHP Secure Pages 0.28Beta	An input validation vulnerability has been reported in PHP Secure Pages that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	phpSecurePages Arbitrary Code Execution CAN-2005-2251	High	Security Tracker, Alert ID: 1014410, July 7, 2005
PHPAuction PHPAuction 2.5	Multiple vulnerabilities have been reported in PHPAuction that could let remote malicious users perform Cross-Site Scripting, SQL injection, or bypass authentication. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPAuction Cross-Site Scripting, SQL Injection, or Authentication Bypassing CAN-2005-2252 CAN-2005-2253 CAN-2005-2254 CAN-2005-2255	High	Security Tracker, Alert ID: 1014423, July 8, 2005
PhpSplash.org PhpSplash 0.8.0	An access control vulnerability has been reported in phpSplash (saveProfile()) that could let remote malicious users hijack user accounts or obtain elevated privileges. Vendor fix issued: http://sourceforge.net/project/showfiles.php?group_id=10566 There is no exploit code required.	phpSlash Account Hijacking or Elevated Privileges CAN-2005-2257	Medium	Secunia, Advisory: SA15936, July 8, 2005
phpWishList phpWishList 0.1.15	A vulnerability has been reported in phpWishList that could let remote malicious users obtain unauthorized administrative access. Vendor fix available: http://sourceforge.net/project/showfiles.php?group_id=121847 There is no exploit code required.	phpWishList Unauthorized Administrative Access CAN-2005-2203	High	Security Tracker Alert ID: 1014432, July 9, 2005
PhpXMail PhpXMail 1.1	A vulnerability has been reported in PhpXMail that could allow a remote malicious user to bypass authentication. No workaround or patch available at time of publishing. There is no exploit code required.	PhpXmail Authentication Bypassing CAN-2005-2183	Medium	Secunia, Advisory: SA15951, July 7, 2005
pngren pngren	An input validation vulnerability has been reported in pngren (kaiseki.cgi) that could let remote malicious users execute arbitrary commands. No workaround or patch available at time of publishing.	pngren Arbitrary Command Execution CAN-2005-2205	High	Security Tracker, Alert ID: 1014426, July 8, 2005

	There is no exploit code required; however, a Proof of Concept exploit has been published.			
Sheddtech PhotoGal 1.5	A vulnerability has been reported in PhotoGal that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PhotoGal Arbitrary Code Execution CAN-2005-2216	High	Security Tracker Alert ID: 1014397, July 6, 2005
Simple PHP Blog Simple PHP Blog 0.4.0	A vulnerability has been reported in Simple PHP Blog that could let remote malicious users obtain the password file. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Simple PHP Blog Password Exposure CAN-2005-2192	Medium	Secunia, Advisory: SA15954, July 8, 2005
SPiD SPiD 1.3.0	A vulnerability has been reported in SPiD that could let remote malicious users include arbitrary files to execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	SPiD Arbitrary File Inclusion CAN-2005-2198	High	Security Focus, 14208, July 11, 2005
Squito Soft Squito Gallery 1.33	An include file vulnerability has been reported in Squito Gallery that could let remote malicious users execute arbitrary commands. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Squito Gallery Arbitrary Commands Execution CAN-2005-2258	High	Security Tracker Alert ID: 1014447, July 11, 2005
USANet Creations MakeBid Deluxe Auction, USANet Shopping Mall, Domain Name Auction, Standard Classified Ads, MakeBid Reverse Auction, MakeBid Standard Auction	An input validation vulnerability has been reported in MakeBid Deluxe Auction, USANet Shopping Mall, Domain Name Auction, Standard Classified Ads, MakeBid Reverse Auction, MakeBid Standard Auction that could let remote malicious users execute commands. Vendor fix available: http://www.usanetcreations.com/updates/index.html There is no exploit code required.	USANet Remote Command Execution CAN-2005-2259	High	Security Tracker, Alert ID: 1014411, July 7, 2005
Xerox Workcentre Pro C2128, C2636, C3545	A vulnerability has been reported in WorkCentre Pro that could let remote malicious users bypass authentication, access files, modify web pages, or perform a Denial of Service. Vendor patch available: http://www.xerox.com/downloads/usa/en/c/cert_P22_NIAP_WCP_C_Only.zip There is no exploit code required.	Xerox WorkCentre Pro Authentication Bypassing, Unauthorized Files Access, Web Page Modification, or Denial of Service CAN-2005-2200 CAN-2005-2201 CAN-2005-2202	Medium	Security Tracker, Alert ID: 1014429, July 8, 2005
WrYBiT PPA 0.5.6	An include flag vulnerability has been reported in PPA that could let remote malicious users execute arbitrary commands. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PPA Arbitrary Command Execution CAN-2005-2199	High	Security Tracker Alert ID: 1014436, July 10, 2005
Zlib Zlib 1.2.2	A buffer overflow vulnerability has been reported in Zlib that could let remote malicious users execute arbitrary code. Updates available, see USCERT Vulnerability Note: http://www.kb.cert.org/vuls/id/680620 Currently we are not aware of any exploits for this vulnerability.	Zlib Arbitrary Code Execution CAN-2005-2096	High	Security Focus, 14162, July 11, 2005 USCERT, Vulnerability Note VU#680620, July 12, 2005

[back to top]

Wireless

The section below contains wireless vulnerabilities, articles, and viruses/trojans identified during this reporting period.

- **New Security Tools Sniff Out WLAN Attacks:** New tools and features from two manufacturers of wireless security software will help network administrators sniff out rogue wireless systems and spot attacks that spread over wireless links. AirDefense Inc. and Newbury Networks Inc. each announced software in the past two weeks that gives administrators new ways to inventory authorized wireless devices; spot attacks; and even spot rogue devices lurking in unsuspected places, a process known as wardriving. Source: http://www.eweek.com/article2/0,1895,1834899,00.asp.

Wireless Vulnerabilities

- **New Wireless "Zero-Day" Attack Discovered:** The security threat of wireless networks to the enterprise keeps growing. The discover of a new wireless attack, "phlooding", targets businesses central authentication server with the goal of overloading it and cause a Denial of Service attack. The "phlooding" attack, discovered by AirMagnet, describes a group of simultaneous but geographically distributed attacks that targets wireless access points with login requests using multiple password combination in what are known as dictionary attacks. Source: http://www.ebcvg.com/articles.php?id=802.

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
July 12, 2005	blogtorrent092.txt	Yes	Proof of Concept exploit for Blog Torrent password disclosure.
July 12, 2005	dragonfly.txt	No	Proof of Concept exploit for Dragonfly Commerce SQL Injection or Price Modification vulnerability.
July 12, 2005	hostingCreate.txt	No	Proof of Concept exploit for Hosting Controller Credit Modification or Account Creation vulnerability.
July 12, 2005	idboard113SQL.txt	No	Proof of concept exploit for Id Board SQL Injection vulnerability.
July 8, 2005	kaiseki.txt	No	Proof of Concept exploit for pngren Arbitrary Command Execution, in kaiseki.cgi, vulnerability.
July 8, 2005	simplephpBlog040.txt	Yes	Proof of concept exploit for Simple PHP Blog Password Exposure vulnerability.
July 7, 2005	aspjarSQL.txt	No	Proof of Concept for ASPJar SQl Injection vulnerability.
July 7, 2005	btftp.txt	Yes	Exploit for Nokia Affix BTFTP Arbitrary Code Execution vulnerability.
July 7, 2005	cartwizMulti.txt	No	Proof of Concept exploit for CartWIZ Cross Site Scripting or SQL Injection vulnerability.
July 7, 2005	comersusMulti.txt	No	Proof of concept exploit for Comersus Cart Cross Site Scripting or SQL Injection vulnerability.
July 7, 2005	dosPlanet.txt	No	Proof of Concept exploit for PlanetFileServer Denial of Service vulnerability.
July 7, 2005	druppy461.pl.txt	Yes	Exploit for Drupal Arbitrary PHP Code Execution vulnerability.
July 7, 2005	eRoomVuln.txt	No	Exploit for the eRoom Plug-In Insecure File Download Handling vulnerability.
July 7, 2005	gnats.txt	Yes	Proof of Concept exploit for GNATS Arbitrary File Overwriting vulnerability.
July 7, 2005	idm405.txt	No	Proof of concept exploit for Internet Download Manager Arbitrary Code Execution vulnerability.
July 7, 2005	iejavaprxyexploit.pl.txt	Yes	Proof of Concept exploit for Microsoft Internet Explorer javaprxy.dll COM object vulnerability.
July 7, 2005	imail.cookie.txt	Yes	Proof of Concept exploit for IMail Password Disclosure vulnerability.
July 7, 2005	kpopper10.txt	No	Exploit for the KPopper Insecure Temporary File Creation vulnerability.
July 7, 2005	McAfeeIPS.txt	No	Proof of Concept exploit for McAfee Security Management System Elevated Privileges or Cross Site Scripting vulnerability.
July 7, 2005	myguestbook_advisory.txt	No	Proof of Concept exploit for MyGuestbook 'Form.Inc.PHP3' Remote File Include vulnerability.
July 7, 2005	pearxmlrpc.pl.txt	Yes	Exploit for the Multiple Vendors XML-RPC for PHP Remote Code Injection vulnerability.
July 7, 2005	phpAuctionMulti.txt	No	Proof of Concept exploit for PHPAuction Cross-Site Scripting, SQL Injection, or Authentication Bypassing vulnerability.
July 7, 2005	phpbb2015.py.txt	Yes	Exploit for the php 2.0.15 viewtopic.php remote command execution vulnerability.
July 7, 2005	phpbb2015dad.txt	Yes	Exploit for the php 2.0.15 viewtopic.php remote command execution vulnerability.
July 7, 2005	phpsource.traverse.txt	No	Proof of Concept exploit for Quick & Dirty PHPSource Printer Directory Traversal vulnerability.
July 7, 2005	phpwebsiteSQL.txt	Yes	Proof of Concept exploit for phpWebSite SQL Injection or Arbitrary Code Execution vulnerability.
July 7, 2005	r57xoops.pl	Yes	Exploit for the Multiple Vendors XML-RPC for PHP Remote Code Injection vulnerability.
July 7, 2005	solsockjack.c	Yes	Proof of Concept exploit for the Solaris SO_REUSEADDR Hijack vulnerability.

July 7, 2005	xmlrpcAnti.pl.txt	Yes	Exploit for the Multiple Vendors XML-RPC for PHP Remote Code Injection vulnerability.

[back to top]

Trends

- **ICANN warns world of domain hijacking:** A report by the internet's leading security experts has warned the world of the risk of domain name hijacking. ICANN's Security and Stability Advisory Committee has outlined several famous and recent thefts of websites, including Panix.com, Hushmail.com and HZ.com, and listed where the system went wrong and what can be done to correct the flaws. Source: http://www.theregister.co.uk/2005/07/12/icann_domain_hijacking/.
- **Zombie bots fuel spyware boom:** Zombie bots such as Gaobot, MyTob and SDbot are often central to the spread of spyware. In just the first and second quarters of 2005, the number of exploited machines using backdoor techniques has increased over 63 per cent from the total at the end of 2004. Source: http://www.theregister.co.uk/2005/07/11/malware_report_mcafee/.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win 32 Worm	Slight Increase	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folders.
2	Zafi-D	Win 32 Worm	Increase	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
3	Mytob.c	Win 32 Worm	Decrease	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
4	Netsky-Q	Win 32 Worm	Slight Decrease	March 2004	A mass-mailing worm that attempts to launch Denial of Service attacks against several web pages, deletes the entries belonging to several worms, and emits a sound through the internal speaker.
4	Mytob-BE	Win 32 Worm	New	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
6	Lovgate.w	Win 32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
6	Netsky-Z	Win 32 Worm	Increase	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.
6	Mytob-AS	Win 32 Worm	New	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
9	Netsky-D	Win 32 Worm	Decrease	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
10	Mytob-EP	Win 32 Worm	New	June 2005	Another slight variant of the mass-mailing worm that utilizes an IRC backdoor and LSASS vulnerability to propagate. Also propagates by email, harvesting addresses from the Windows address book.

Table Updated July 11, 2005

Viruses or Trojans Considered to be a High Level of Threat

- **Targeted Trojan Email Attacks:** The United States Computer Emergency Readiness Team (US-CERT) has received reports of an email based technique for spreading trojan horse programs. A trojan horse is an attack method by which malicious or harmful code is contained inside apparently harmless files. Once opened, the malicious code can collect unauthorized information that can be exploited for various purposes, or permit computers to be used surreptitiously for other malicious activity. The emails are sent to specific individuals rather than the random distributions associated with a phishing attack or other trojan activity. Source: Technical Cyber Security Alert TA05-189A, http://www.us-cert.gov/cas/techalerts/TA05-189A.html.

[back to top

Last updated